Dr.WEB®
Mobile Security Suite

Защити созданное

Курс DWCERT-030-12
Современные угрозы для мобильных устройств

План курса

1. Криминальная индустрия производства вредоносных программ
2. Вредоносные программы для ОС Android
3. А есть ли вредоносные программы для мобильных устройств «в дикой природе»?
4. Как вредоносные программы проникают на мобильные устройства?
5. Почему для защиты мобильного устройства только антивируса недостаточно?
6. Информационные ресурсы о «мобильных» угрозах.

1. Криминальная индустрия производства вредоносных программ

Уже давно прошло то время, когда создателями вредоносного ПО были программисты-одиночки. Современные вредоносные программы разрабатываются не просто вирусописателями-профессионалами — это хорошо организованный криминальный бизнес, вовлекающий в свою преступную деятельность высококвалифицированных системных и прикладных разработчиков ПО.

Структурные элементы некоторых преступных сообществ

В ряде случаев роли злоумышленников внутри преступных сообществ могут быть разделены следующим образом:

1. **Организаторы** — лица, которые организуют процесс создания и использования вредоносного ПО и руководят им. Созданное вредоносное ПО организаторы могут либо использовать сами, либо продавать другим преступникам или их объединениям.

2. **Участники**:

- Разработчики вредоносного ПО
- Тестировщики созданного ПО
- Исследователи уязвимостей в операционных системах и прикладном ПО в преступных целях
- «Специалисты» по использованию вирусных упаковщиков и шифрованию
- Распространители вредоносного ПО, специалисты по социальной инженерии
- Системные администраторы, обеспечивающие распределенную безопасную работу внутри преступного сообщества и управление бот-сетями

Такая «организация труда» позволила криминальным группировкам организовать тестирование разрабатываемых ими вредоносных программ на необнаружение всеми актуальными антивирусными решениями. Тестирование создаваемого вредоносного ПО на актуальных версиях антивирусов позволяет злоумышленникам внедрять на компьютеры и мобильные устройства вирусы и троянцев в обход антивирусной защиты. Ни одна антивирусная программа, как бы она ни была хороша в тестах на обнаружение «заразы» эвристическими механизмами, не сможет ничего в этом случае сделать.

Также все чаще криминальные группировки создают «таргетированные» угрозы — вредоносные программы, разработанные для заражения конкретных, относительно небольших групп ПК или мобильных устройств (например, пользователей одного банка). Как правило, это качественно написанные вредоносные программы, не оказывающие существенного влияния на работу зараженных машин и в момент заражения не опознаваемые средствами защиты, что позволяет данным вредоносным программам оставаться необнаруженными в течение длительного времени.

В результате перехода к «промышленным» методам распространения вредоносных программ в «дикую природу» выпускаются только те из них, которые не обнаруживаются антивирусами, – даже с помощью эвристических механизмов, пока не получены обновления. **Это привело к резкому росту количества необнаруживаемых на момент проникновения вредоносных программ.**

2. Вредоносные программы для ОС Android

Больше всего вредоносных программ создается для инфицирования мобильных устройств под управлением операционной системы Android. На это влияет:

- широкая распространенность платформы: по данным на 2013 год Android установлена на 80% мобильных устройств во всем мире;
- открытый исходный код, позволяющий злоумышленникам исследовать его в поисках уязвимостей;
- возможность установки приложений из произвольных (не всегда доверенных) источников;
- несвоевременное обновление ПО и версий прошивок некоторыми производителями устройств.

Что могут вредоносные программы для ОС Android?

Современные телефоны, смартфоны и планшеты, оснащенные полноценными операционными системами с огромными возможностями, являются соблазнительными целями для хакерских атак. Об этом свидетельствует постоянный рост количества поступающих в антивирусную лабораторию Dr.Web новых вредоносных программ, нацеленных на мобильные системы.

Мобильные устройства предоставляют киберкриминалу куда больше возможностей, чем обычные компьютеры. Многие из них оборудованы камерами. В любом телефоне есть микрофон. В некоторых имеются GPS-приемники. Все это прекрасно помогает в различных жизненных ситуациях, пока мобильное устройство контролирует его владелец. Но если контроль над устройством перехвачен злоумышленником, он получает следующие возможности.

- **Получать доступ к почте и хранящимся на устройстве конфиденциальным данным**, в том числе похищать пароли жертвы (например, к системам «Клиент-Банк» или аккаунтам социальных сетей), номера банковских счетов и многое другое. Это дает возможность для шантажа, сбора и перепродажи информации о жертве или подмены информации (Android.AntaresSpy.1, Android.SmsSpy).

Мобильные устройства используются людьми и для работы. Сотрудники работают в дороге и дома, хранят корпоративные данные на личных устройствах, заходят на корпоративные ресурсы с личных устройств. **Поэтому так опасна кража данных и паролей доступа с личных мобильных устройств.**

- **Блокировать некоторые функции телефона или удаленно управлять им** — например, перехватывать входящие СМС, нежелательные для преступников, — это может использоваться с целью вредительства или для вывода сотрудника конкурента из строя в нужный момент (Android.Wukong, Android.SmsSpy, Android.Gongfu).
- **Отправлять без ведома пользователя сомнительные СМС и совершать звонки на премиум-номера** — т. е. наносить прямой денежный ущерб (Android.SmsSend, Android.SmsBot).
- **Совершать хищения** — с банковского счета, из систем онлайн-платежей.
- **Шпионить** — записывать разговоры жертвы через включенный микрофон; получать данные от GPS-навигатора о местонахождении (присутствии или отсутствии в определенных местах); включать фото- и видеокамеру устройства с целью выяснить, где находится владелец устройства; следить за тем, какие сайты посещает жертва, кому звонит и кто звонит ей, с кем ведет переписку, кому отправляет СМС.

Банковские троянцы для мобильных устройств

На данный момент наиболее опасны программы, перехватывающие СМС с mTAN-кодами, которые многие банковские институты используют для подтверждения финансовых операций.

Примеры

- **Банковский троянец Android.SpyEye.1 и его версия для ПК.** При обращении к различным банковским сайтам, адреса которых присутствуют в конфигурационном файле троянца, в просматриваемую пользователем веб-страницу встраивается постороннее содержимое (текст или веб-формы для ввода данных). Ничего не подозревающая жертва загружает в браузере веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «Банк-Клиент», с предложением загрузить на мобильный телефон специальное приложение, на самом деле содержащее троянскую программу-шпиона.
- **Программа для перехвата СМС-сообщений Android.Pincer.** Вредоносная программа распространяется под видом сертификата безопасности, который якобы требуется установить на Android-устройство. В случае если неосторожный пользователь выполнит установку и попытается запустить троянца, Android.Pincer продемонстрирует ложное сообщение об успешной установке сертификата. При очередном включении мобильного устройства Android.Pincer подключается к удаленному серверу злоумышленников и загружает на него ряд сведений о мобильном устройстве. Android.Pincer дает возможность использовать вредоносную программу как инструмент для проведения целевых атак, в том числе красть специфические СМС-сообщения с указанных номеров, например, сообщения от систем «Банк-Клиент», содержащие проверочные mTAN-коды.
- **Android.Fakealert** – семейство вредоносных программ, выдающих себя за антивирусные приложения для ОС Android и сообщающих об обнаружении вирусных угроз, за устранение которых необходимо заплатить.
- **Android.Spy** – многофункциональные троянцы-шпионы. Обладают возможностью чтения и записи контактов, приема и отправки СМС-сообщений, определения GPS-координат, чтения и записи закладок браузера, получения сведений об IMEI мобильного устройства и номере мобильного телефона. Имеется функционал для осуществления специализированного веб-поиска и перехода по определенным ссылкам в браузере.
- **Android.DownLoader** – троянские программы, предназначены для загрузки и установки других вредоносных приложений на мобильные устройства под управлением ОС Android.
- **Android.Backdoor** – семейство троянских программ, заражающих мобильные устройства под управлением ОС Android и предназначенных для выполнения поступающих от злоумышленников команд.
- **Android.Basebridge** – троянцы этого семейства способны выполнять отправку и перехват входящих СМС-сообщений, отправлять на удаленный сервер информацию о мобильном устройстве, а также устанавливать на него другие вредоносные приложения.

Для более подробного изучения темы вирусов для мобильных рекомендуем ознакомиться с обзором Android-угроз за 2012 год, подготовленным специалистами «Доктор Веб».

3. А есть ли вредоносные программы для мобильных устройств «в дикой природе»?

К сожалению, вредоносные программы для Android действительно существуют и представляют реальную опасность для пользователей в разных странах мира.

Анализ собранной с использованием Антивируса Dr.Web для Android статистики показал:

- **в сентябре 2013 года** пользователи запускали сканирование около 17 000 000 раз, при этом наличие вредоносного или сомнительного ПО было зафиксировано более 4 000 000 раз.
- **в октябре 2013 года** было зафиксировано около 11 миллионов срабатываний антивирусного монитора Dr.Web для Android, более 4 миллионов угроз для Android было обнаружено в процессе сканирования.

Наиболее распространенные угрозы для операционной системы Android:

- троянцы семейства **Android.SmsSend**;
- троянцы семейства **Android.SmsSpy**;
- программы-шпионы семейства **Android.Spy**.

Кроме того, весьма распространены троянские программы **Android.DownLoader**, **Android.Backdoor**, **Android.Gingersploit**, **Android.Basebridge** и **Android.Fakealert**, а также всевозможные рекламные инструменты, например, not a virus Tool.SMSSend, not a virus Tool.Rooter и not a virus Adware.Airpush.

4. Как вредоносные программы проникают на мобильные устройства?

1. **Через уязвимости.** Уязвимостью называют недостаток в системе или прикладном ПО, используя который можно нарушить их целостность (иными словами, проникнуть в них) и вызвать неправильную работу. Теоретически абсолютно любую ошибку в программе можно использовать для причинения вреда системе в целом.

Не существует ПО, в котором не было бы уязвимостей. Но особенно много уязвимостей в операционных системах Windows и Android — первая наиболее распространена для компьютеров и ноутбуков, вторая — для мобильных устройств.

Разработчики программного обеспечения прилагают усилия по закрытию уязвимостей, особенно критических, но вирусописатели часто узнают об уязвимостях раньше, чем разработчики этого ПО (это так называемые уязвимости нулевого дня — 0day exploits, уязвимости, о которых пока известно только вирусописателю или для исправления которых производитель ПО пока еще не выпустил «заплатки»).

Чтобы устранять уязвимости (закрывать бреши безопасности), пользователю надо своевременно **обновлять установленное на мобильном устройстве ПО** — все без исключения программы, а не только антивирус.

1. **Из сети Интернет.** Многие сайты, независимо от содержимого, могут содержать вирусы или вредоносные скрипты. **Заражение может происходить при посещении сайта**, когда злоумышленники различными способами заставляют пользователя скачать и запустить apk-файл.

Удивительный факт

Сайты, которые чаще всего являются источниками вредоносного ПО и фишинговых атак

- Сайты, посвященные технологиям и телекоммуникациям
- Бизнес-сайты: бизнес-СМИ, порталы деловых новостей, бухгалтерские сайты и форумы, интернет-курсы/лекции, сервисы для повышения эффективности бизнеса
- Порнографические сайты и ресурсы для скачивания «халявных» программ

Именно через них (предварительно взломав) злоумышленники чаще всего «подкарауливают» своих жертв, перебрасывая их на зараженные ресурсы. Пиратские дистрибутивы программ тоже с высокой долей вероятности могут быть носителями вирусов или троянцев.

2. **Через мобильные редиректы**

Даже если вы убеждены, что посещаемые вами с использованием мобильных устройств сайты хорошо вам известны и абсолютно безопасны, подобная уверенность может обернуться существенными финансовыми потерями. Значительная часть интернет-сайтов работает при помощи так называемых систем управления контентом (Content Management Systems, CMS) — это специальный набор программ,

позволяющих публиковать веб-страницы, редактировать их содержимое, гибко настраивать оформление и оперативно менять структуру сайта. Большинство современных CMS распространяется согласно условиям открытых лицензий, то есть бесплатно, при этом любой желающий может ознакомиться с их исходным кодом. Благодаря этому злоумышленники, изучив структуру составляющих CMS программ, могут отыскать в них уязвимости и взломать работающий под управлением такой системы сайт.

С помощью взломанных сайтов злоумышленники могут распространять различные вредоносные программы, самыми «популярными» из которых являются различные модификации Android.SmsSend. Троянцы этого семейства предназначены для отправки СМС-сообщений с повышенной тарификацией и подписки пользователей на различные платные контент-услуги и сервисы, в результате чего с абонентского счета может списываться определенная сумма.

По подсчетам специалистов компании «Доктор Веб», в российском сегменте Интернета порядка 3% веб-сайтов перенаправляют пользователей мобильных смартфонов и планшетов на базе Android на вредоносные интернет-ресурсы, распространяющие опасное ПО. Это означает, что более 45 000 сайтов могут заразить Android-устройства различными троянскими программами, а с учетом мошеннических и фишинговых ресурсов их общее количество может достигать от 100 до 200 тысяч.

Специальный бесплатный сервис «**УРоЛог Dr.Web**» позволяет проверить ссылку на мобильный редирект и предупредить об опасности. Особенно это актуально для тех, кто еще не установил антивирус на свое мобильное устройство.

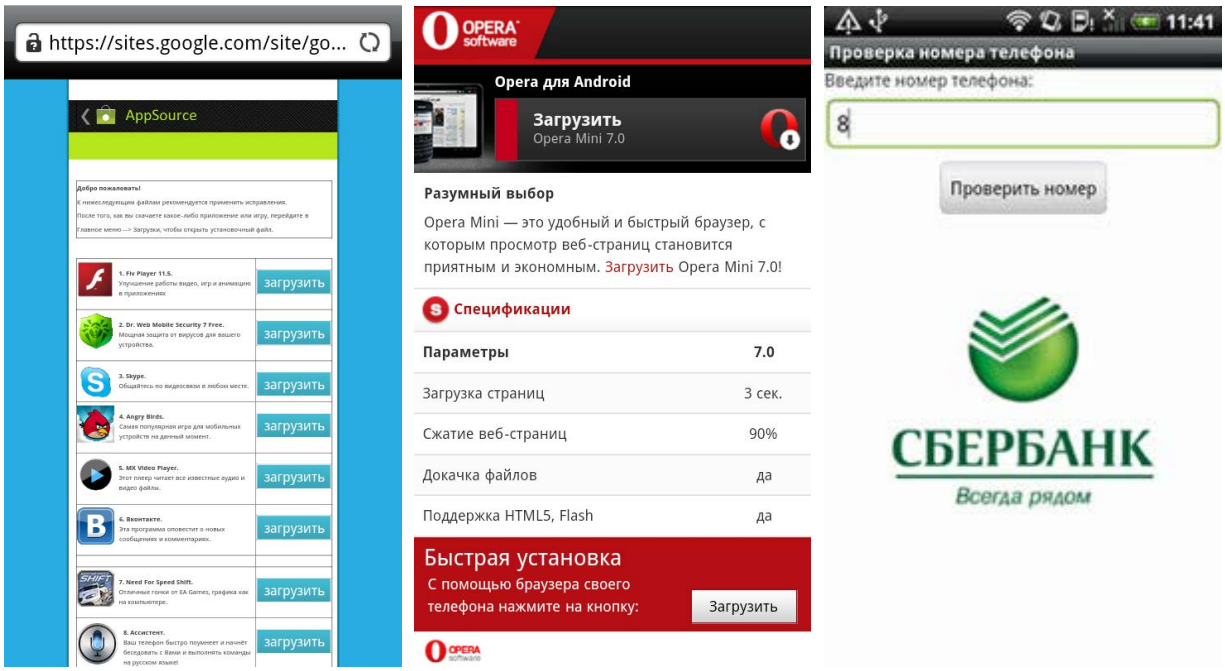
3. Благодаря фишингу и социальной инженерии

Серьезную опасность для пользователей Android-устройств представляют и фишинговые атаки, при помощи которых киберпреступники пытаются обманным путем заставить своих жертв выдать конфиденциальные сведения (логины, пароли, телефонные номера и т. п.), совершить сомнительные действия (например, перевести определенную сумму с банковской карты), либо установить вредоносную программу. Для этого мошенники могут использовать:

- веб-сайты, имитирующие внешний вид и функционал настоящих ресурсов (почтовых сервисов, банков, онлайн-магазинов, социальных сетей);
- СМС-сообщения, отправленные якобы от имени банков, крупных компаний, государственных структур;
- троянские приложения, которые похожи на оригинальные программы, но под надуманным предлогом требующие, например, ввода конфиденциальных сведений.

Попавшись на уловку сетевых мошенников, вы можете лишиться не только доступа к любимым онлайн-сервисам, но и, что немаловажно, рискуете потерять все свои деньги!

Примеры фишинговых сайтов



4. **Благодаря самим пользователям.** Даже если вредоносная программа не умеет использовать уязвимости для проникновения, пользователи всегда готовы прийти ей на помощь.

Большая часть современных вредоносных программ не является вирусами — т. е. не имеет механизма саморазмножения. Они рассчитаны на распространение самими пользователями. С помощью разнообразных уловок (методов социальной инженерии) преступник добивается, чтобы жертва установила какую-либо вредоносную программу, открыла вредоносный файл, посетила взломанный сайт и т. д.

Так, например, **Android.Plankton**, позволявший осуществлять сбор и передачу информации о зараженном устройстве, был вручную загружен пользователями 150 000 раз (!) с официального Android Market (прежнее название Google Play), прежде чем был удален администрацией портала.

5. Почему для защиты мобильного устройства только антивируса недостаточно?

Антивирус защитит от вирусов и вредоносных программ, в частности троянцев. **Но сегодня этого уровня защиты уже недостаточно.**

Только комплексное антивирусное решение, например, **Dr.Web для Android** позволит защититься от всех типов вредоносного ПО, используемого мошенниками для совершения киберпреступлений. В его состав должны входить антивирус, антиспам, антивор и URL-фильтр.

- **Антиспам** защитит от нежелательных сообщений и звонков.
- **Антивор** поможет найти мобильное устройство в случае его утери или кражи, заблокировать его и при необходимости дистанционно удалить конфиденциальную информацию. Мобильные устройства подвержены огромному риску потери или кражи. Информация (включая пароли и логины доступа) может оказаться в нечистоплотных руках. Один лишь антивирус не может защитить ее, если злоумышленник или обычный человек, нашедший устройство, захочет ознакомиться с содержимым находки.
- **URL-фильтр** ограничит доступ к потенциально опасным сайтам. Он особенно полезен, если устройством пользуется ребенок, который пока еще не осознает опасности посещения тех или иных ресурсов.

ВАЖНО!

Некоторые производители антивирусов заявляют о наличии в составе их продуктов для защиты ОС Android компонента Родительского контроля.

Создать полноценный Родительский контроль для этой операционной системы в данный момент НЕВОЗМОЖНО.

Базовые настройки стандартного браузера Android и браузера Google Chrome для Android не позволяют использовать Родительский контроль в полном смысле этого слова, т. к. любой пользователь может открыть страницу в анонимном режиме, и никакое ПО не сможет отследить его действия.

Поэтому, в отличие от конкурентов, «Доктор Веб» не позиционирует URL-фильтр Dr.Web Cloud Checker как Родительский контроль.

6. Информационные ресурсы о «мобильных» угрозах.

- Новости о мобильных угрозах
- Онлайн-сервис УРоЛог Dr.Web — проверка интернет-ссылок на т.н. «мобильные редиректы»
- Вирусная библиотека